ABSTRACT

Improved security processing circuits are discussed which may be used alone or as part of a network interface device of a host system using a DES engine to accomplish 3DES processing. The security processing circuit is adapted for selectively encrypting outgoing data and decrypting incoming data, where the network interface device may be fabricated as a single integrated circuit chip. The improved circuit makes use of a unique circuit component arrangement to provide shortened path timings within the DES engine processing. To accomplish this overall timing performance improvement, the permutation and inverse permutation blocks are removed from these critical path timings of the three individual DES processing operations, and moved to the beginning and end of the 3DES process. Methods are also provided for performing 3DES encryption and decryption services between the host system and a network, in which security information is obtained from the host system, which is used together with a set of secret keys for 3DES processing data utilizing an intermediate result fed back to the DES engine of the 3DES IPsec circuit.